University of North Carolina Asheville
Identity Theft Prevention Program

Program Adoption

As a best practice and using as a guide the Federal Trade Commission's ("FTC") Red Flags Rule, implementing Section 114 of the Fair and Accurate Credit Transactions Act of 2003, University of North Carolina Asheville developed this Identity Theft Prevention Program. This Program was developed with oversight and approval of the University of North Carolina Asheville Board of Trustees. After consideration of the size and complexity of the University's operations and account systems, and the nature and scope of the University's activities, the University of North Carolina Asheville Board of Trustees determined that this Program was appropriate for the University, and therefore approved this Program on June 18, 2009.

The purpose of the program is to detect, prevent and mitigate identity theft in connection with any covered account. This program envisions the creation of policies and procedures in order to achieve these goals.

Definitions

"Covered Account" means

- Any account that constitutes a continuing financial relationship or is designed to permit multiple payments or transactions between the University and a person for a service, such as extension of credit, debit cards, Perkins Loans, FFELP, institutional loans, HIPAA covered accounts, deposit accounts, scholarship accounts, and the like.
- Any other account the University offers or maintains for which there is a reasonably foreseeable risk to holders of the account or to the safety and soundness of the University from Identity Theft, such as use of consumer reports for employee background checks or applicants for credit, institutional debit card applications, and the like.

"Identifying Information" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including, but not limited to:

- name
- address
- telephone number
- social security number
- date of birth
- government-issued driver's license or identification number
- alien registration number
- government passport number
- employer or taxpayer identification number
- individual identification number including insurance identification numbers
- computer's Internet Protocol address
- bank or other financial account routing code

"Identity Theft" means a fraud committed or attempted using the Identifying Information of another person without authority.

"Program Administrator" means the individual designated with primary responsibility for oversight of the Program.

"Red Flag" means a pattern, practice, alert or specific activity that indicates the possible existence of Identity Theft.

"Service Provider" means a person or entity that provides a service directly to the University.

Identification of Red Flags

In order to identify relevant Red Flags, the University considers the types of Covered Accounts it offers or maintains, the methods it provides to open its Covered Accounts, the methods it provides to access its Covered Accounts, and its previous experiences with Identity Theft.

Red Flags may be detected while implementing existing account opening and servicing procedures such as: individual identification, caller authentication, third party authorization, and address changes.

The University identifies the following Red Flags in each of the listed categories:

- Notifications and Warnings from Consumer Reporting Agencies
    - Report of fraud accompanying a credit report;
    - Notice or report from a credit agency of a credit freeze on an applicant;
    - Notice or report from a credit agency of an active duty alert for an applicant;
    - Receipt of a notice of address discrepancy in response to a credit report request; and
    - Indication from a credit report of activity that is inconsistent with an applicant's usual pattern or activity.
- Suspicious Documents
    - Identification document or card that appears to be forged, altered or inauthentic;
    - Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
    - Other document with information that is not consistent with existing individual information; and
    - Application for service that appears to have been altered or forged.
- Suspicious Personal Identifying Information

- Identifying Information presented that is inconsistent with other information the individual provides (example: inconsistent birth dates);
- Identifying Information presented that is inconsistent with other sources of information (example: an address not matching an address on a loan application);
- Identifying Information presented that is the same as information shown on other applications that were found to be fraudulent;
- Identifying Information presented that is consistent with fraudulent activity (examples: an invalid phone number or fictitious billing address);
- Social security number presented that is the same as one given by another individual;
- An address or phone number presented that is the same as that of another person;
- A person fails to provide complete personal Identifying Information on an application when reminded to do so; and
- A person's Identifying Information is not consistent with the information that is on file for the individual.

- Suspicious Covered Account Activity

  - Change of address for an account followed by a request to change the individual's name;
  - Payments stop on an otherwise consistently up-to-date account;
  - Account used in a way that is not consistent with prior use;
  - Mail sent to the individual is repeatedly returned as undeliverable;
  - Notice to the University that an individual is not receiving mail sent by the University;
  - Notice to the University that an account has unauthorized activity;
  - Breach in the University's computer system security; and
  - Unauthorized access to or use of individual account information.

- Alerts from Others

  - Notice to the University from an individual, Identity Theft victim, law enforcement or other person that the University has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

Detection of Red Flags

- Student Enrollment

In order to detect any of the Red Flags identified above associated with the enrollment of a student, University personnel shall take the following steps to obtain and verify the identity of the person opening the account:

- Require certain Identifying Information such as name, date of birth, academic records, home address or other identification; and
- Verify the individual's identity at time of issuance of individual identification card (review of driver's license or other government-issued photo identification).

- Existing Accounts

In order to detect any of the Red Flags identified above for an existing Covered Account, University personnel shall take the following steps to monitor transactions on an account:

  - Verify the identification of individuals if they request information (in person, via telephone, via facsimile, via email);
  - Verify the validity of requests to change billing addresses by mail or email and provide the individual a reasonable means of promptly reporting incorrect billing address changes; and
  - Verify changes in banking information given for billing and payment purposes.

- Consumer ("Credit") Report Requests

In order to detect any of the Red Flags identified above for an employment or volunteer position for which a credit or background report is sought, University personnel shall take the following steps to assist in identifying address discrepancies:

  - Require written verification from any applicant that the address provided by the applicant is accurate at the time the request for the credit report is made to the consumer reporting agency; and
  - In the event that notice of an address discrepancy is received, verify that the credit report pertains to the applicant for whom the requested report was made and report to the consumer reporting agency an address for the applicant that the University has reasonably confirmed is accurate.

Response to Red Flags

- Once potentially fraudulent activity is detected, an employee must act quickly, because a rapid appropriate response can protect individuals and the University from damages and loss. At a minimum, the employee must gather all related documentation, write a description of the situation, and present this information to the Program Administrator. This should occur no later than five business days after detection of potentially fraudulent activity or sooner if the circumstances require.

- The Program Administrator will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.

- If a transaction is determined to be fraudulent, appropriate actions must be taken immediately. Actions may include:
  - Canceling the transaction;
  - Notifying and cooperating with appropriate law enforcement;
  - Determining the extent of liability of the University; and
  - Notifying the actual individual upon whom fraud has been attempted.

Prevention and Mitigation of Identity Theft

In the event University personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending on their determination of the degree of risk posed by the Red Flag:

- Prevent and Mitigate

    - Continue to monitor a Covered Account for evidence of Identity Theft;
    - Contact the individual or applicant (for which a credit report was run);
    - Change any passwords or other security devices that permit access to Covered Accounts;
    - Refuse to open a new Covered Account;
    - Provide the individual with a new individual identification number;
    - Notify the Program Administrator for determination of the appropriate step(s) to take;
    - Notify law enforcement;
    - File or assist in filing a Suspicious Activity Report ("SAR") with the Financial Crimes Enforcement Network, United States Department of the Treasury; or
    - Determine that no response is warranted under the particular circumstances.

- Protect Identifying Information

In order to further prevent the likelihood of Identity Theft, the University will take the following steps with respect to its internal operating procedures to protect individual Identifying Information:

    - Provide clear notice on authenticated websites that the site is secure or is not secure;
    - Clearly articulate that paper documents and computer files no longer needed will be disposed of properly. Clearly articulate what the disposal methods will be.
    - Complete the implementation of Network Access Control so that office computers with access to Covered Account information are password protected;
    - Clearly articulate how university laptops should be secured and take advantage of emerging technologies to move toward whole disk encryption;
    - Avoid the use of social security numbers when possible;
    - Provide for the security of the physical facility that contains Covered Account information;
    - Clearly articulate the secure methods of electronic transmission of sensitive information and develop guidelines to help ensure that transmission is limited to what is necessary for the business functions of the institution;
    - Ensure automatic computer virus protection is up to date; and
    - Require and keep only the kinds of individual information that are necessary for University purposes.

Additional Identity Theft Prevention Measures

- Hard Copy Distribution

Each employee and contractor performing work for the University will comply with the following policies:

- File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with Identifying Information will be locked when not in use.
- Storage rooms containing documents with Identifying Information and record retention areas will be locked at the end of each workday or when unsupervised.
- Desks, workstations, work areas, printers and fax machines, and common shared work areas will be cleared of all documents containing Identifying Information when not in use.
- Whiteboards, dry-erase boards, writing tablets, and other writing surfaces in common shared work areas will be erased, removed, or shredded when not in use.
- When documents containing Identifying Information are discarded, they will be placed inside a locked shred bin or immediately shredded using a mechanical cross cut or Department of Defense-approved shredding device. Locked shred bins are labeled "Confidential paper shredding and recycling."

- Other Policies and Procedures

This Program incorporates by reference the following internal policies and procedures:

Approved Administrative Information Technology Policies Usage Policies

- Student Computing and Networking Usage Policy - www.unca.edu/policies/71.pdf
- Faculty/Staff Computing and Networking Usage Policy - www.unca.edu/policies/72.pdf
- Access to Information Resources and Data - www.unca.edu/policies/75.pdf
- Web Resource Management - www.unca.edu/policies/77.pdf
- Network Security - www.unca.edu/policies/78.pdf

Information Technology Policies under development

- Data Classification and Usage

http://www.unca.edu/compcenter/policies/internal/data_classification/index.asp

- Web Content Guidelines

http://www.unca.edu/compcenter/policies/internal/WebContentGuidelines/index.asp

Personnel Records Policy (pending Senor Staff Approval)

- Confidential Information

Agreement of Confidentiality

- Human Resources Department Agreement of Confidentiality Form

Program Administration

- Oversight

    - Responsibility for developing, implementing and updating this Program lies with the University's Program Administrator; responsibility for approving the Program lies with the University's Board of Trustees.
    - The Program Administrator shall be responsible for ensuring appropriate training of University staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.

- Staff Training

University employees responsible for implementing the Program shall be trained under the direction of the Program Administrator in the detection of Red Flags and the responsive steps to be taken when a Red Flag is detected.

- Reports

Appropriate staff shall report to the Program Administrator at least annually on compliance by the University with this Program. The report shall address matters such as the effectiveness of the policies and procedures of the University in addressing the risk of Identity Theft in connection with the opening of Covered Accounts and with respect to existing Covered Accounts; Service Provider arrangements; significant incidents involving Identity Theft and the University's response; and recommendations for material changes to the Program.

- Service Provider Arrangements

In the event the University engages a Service Provider to perform an activity in connection with one or more Covered Accounts, the University will take the following steps to ensure the Service Provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of Identity Theft.

    - Require, by signed contract, that Service Providers have such policies and procedures in place; and
    - Require, by signed contract, that Service Providers review the University's Program and report any Red Flags to the Program Administrator.

- Program Updates

The Program Administrator shall review and update this Program at least annually to reflect changes in risks to individuals and the soundness of the University from Identity Theft. In doing so, the Program Administrator shall consider the University's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, and changes in the University's business arrangements with other entities.